Unruly Innovation: Distributed Ledgers, Blockchains and the Protection of Transactional Rents

We present a new conceptual model of disruptive innovation and apply it to the emerging financial technology of distributed ledgers and smart contracts. Our analysis illustrates the new features of this technology and why there is an argument that, in several respects, the combination of distributed ledger technology and cryptographically enabled contracts changes the economic framework within which individuals, firms and policy makers reside. This foundational level of disruption appears to have several new features, more notably a fundamental change in the game played by economic actors: the ability to self-deregulate. The paper clarifies these complex interactions and illustrates the main points using a recent case study from the Distributed Autonomous Organizations of the Ethereum project as well from a mathematical standpoint. Automation and distribution with powerful computing languages boost the speed of seizing opportunities as well as of tripping into (in-eliminable) severe risks.

Key words: Disruptive Innovation; Combinatorial Innovation; Smart Contracts; Crypto currencies; Theory of the firm and creation; FinTech.

---

1. Introduction

> "Unruly. adjective. Disorderly and disruptive *and* not amenable to discipline or control." Oxford English Dictionary, 2016 (Our emphasis).

Distributed ledgers combined with cryptographically enabled programs to operate on such ledgers (smart contracts) permit the ad-hoc creation of virtual organizations that ascribe ownership rights on virtual assets with almost limitless flexibility. This ability to program organizations able to run on anonymous end points and open hardware without recourse to existing legal frameworks opens up a universe of innovation possibilities for Financial Technology (FinTech), with very low transactions costs and high levels of flexibility. One of the earliest financial application of distributed ledgers was just distributed payment systems such as Bitcoin (Nakamoto 2008). In time, more sophisticated technologies have emerged to capture key financial components such as Exchanges. For instance, Massacci et al. (2017a) illustrates a market structure with auctions, clearing, trading and settlement of

contingent claims: the ledger technology is mixed with many different types of cryptographic technologies that provide evidence of position for participants, whilst tracking the solvency of each individual and the market as a whole. This type of organizational construction has several hundreds of individual components. Typically, modular technologies of this type have enabled periods of sustained and innovative growth that often disrupts existing incumbents (disruptive innovation). Yet, we argue in this paper that this type innovation proffers both a fascinating example of how technology can facilitate innovation in FinTech but expose organizations to new risks *not present* in traditional markets.

Whilst Massacci et al. (2017a) finely specified such FinTech constructions to prove the equivalence with a centralized Exchange platform, several other distributed platforms (e.g. Ethereum, Nexos, etc.) propose themselves as vehicles for arbitrary constructions by making full use of expressive programming languages (Turing-Complete) to encode smart contracts. This definitely allows for a great degree of flexibility. However, to be Turing complete the programming language used to implement the nexus of contracts enshrines a level of complexity such that in the worst case the only way to understand its outcomes is to execute the program itself. For sufficiently expressive programs, e.g. with dynamic generation and evaluation of fragments of the code, unintended states of nature may occur by mistake or mischief. From an ethical viewpoint[1], those states may be demonstrably unfair. However, as pointed by Lessig (1999), in a distributed scenario there is no legal framework to resolve disputes surrounding the initial intentions at incorporation. The code itself determines the authentic interpretation of its alleged specifications by being jury, judge and executioner. We argue that there is a need to both disentangle and re-integrate these concepts to appropriately model the impacts of these new technologies for FinTech, given their role as both a 'product' and a 'legal framework' for the creation, management and destruction of quasi firm-like entities.

The contribution of this paper is to introduce this new notion of unruly innovation and document the implications on FinTech technology both with a qualitative case study as well as with a mathematical interpretation. To our knowledge this is the first paper to synthesize these

[1] Using the legal concept of the viewpoint of the 'resonable-ness' of an average person representing society.

areas.

1.1. A Primer on the Underpinning Technologies

The underpinning technologies that drive this new medium are *distributed ledger technologies* (DLTs for short), block-chains and cryptocurrencies. DLTs are databases that are distributed across a large number of computing nodes in some form of network. The interesting feature of a DLT is that no one component of the network controls the overall information on the DLT, but can dynamically query it. This technology allows a ledger to be maintained that tracks transactions and attempts to ensure that no (small) group of individuals can subvert the ledgers' integrity.

The ledger can record almost any information, but the commonest example of a financial use is in maintaining a 'block-chain'. This is a systematically updated record of transactions that allows the ledger to allocate debits and credits and to ensure that some desired properties are maintained (for instance no double spending and no improper routing of finances).

The values recorded in the transactions can be provided by a central bank, as recently proposed by Danezis and Meiklejohn (2015), exchanged with commodities or other existing currencies (Ripple Labs 2015) or created by engaging in a specific action such as solving hard computational problems such as proof of work (Nakamoto 2008). The key issue is that no single machine or individual entity controls the distributed ledger (so that potentially all entities have a copy of it and hence the term distributed) and all participating entities run protocols that guarantee the security, integrity and coherence of the distributed copies through "Byzantine Fault Tolerance", (i.e. where a minority of actors can behave in arbitrary ways). Essentially, if a ledger obeys these mathematical principles it should be highly unlikely that an individual or group of individuals coordinating could corrupt the ledger for financial gain, or commit economic injury to the other members, (Ben-Or 1983, Lynch 1989, Castro and Liskov 2002).

In the first instance, this innovation aims to replace standard payment transaction networks, this includes cash, but more importantly real time gross settlement (RTGS) of centrally banked money. Whilst some limitations exist on transaction volumes, frameworks built around DLTs are generally simple to scale as individual participants can choose to migrate to a technology

if the marginal benefit exceeds marginal cost, with very low fixed costs. In this respect, block chains are not overly different from the disruptive technologies based around the development of the rigid disk drive discussed by Christensen (1993) or Christensen et al. (1998).

However, our interest focuses on the next stage developments in the arena of DLTs and block chains, that of *cryptographically enabled contracts*, sometimes referred to as *smart contracts* that replicate normal contracts but correspond to i) executable pieces of code, ii) enforceable through a cryptographically enable ledger.

In this instance, the financial value of the contract (either through some proof or work, or proof of initial capital exchange) is assigned as a property right subject to specific rules. Recombination of these contracts into a nexus can be used to form contractual entities that resemble firms and markets. We argue that this property provides a more fundamental form of disruptive innovation where incumbents are more than simply firms in a particular market, as it challenges the very notion of a firm as a legal entity and the legal medium that enables contract enforcement.

1.2. The Underlying Unruliness of the Technology

A foundational point in the disruption literature focuses on the notion of an innovation, be it a technology or some more abstract innovation concept, that comes to replace existing offerings or frameworks and requires incumbents to adapt/resist or be replaced by new entrants, see Markides (2006) for an introspection on the various modelling frameworks in this area, or Christensen (1993), Christensen et al. (1998) for a proposed simple typology (sustaining versus disruptive technologies). Whilst the ideas from Christensen (1993) have proven controversial and provoked considerable debate in the innovation literature, this debate has centered on the notion of a company as the innovation nexus.

We argue that the types of new technologies discussed herein, re-center this argument and hence, the notion of disruption. The founding notion of a firm lies in the ability to make contracts, either implicitly (under the shadow of the future) or more usually explicitly as a series of enforceable agreements backed by a legal process (often by a civil process that enacts torts or delicts, that remediate breaches of the terms of reference). The state, as a notional actor, provides the legal medium that guarantees the appropriate redistribution of

value and rights to the appropriate individuals.

The notion of firms as legal entities formed by a nexus of contracts underpins the concept of a commercial organization in respect to the modern economy. Whilst companies and related organizations, such as NGOs, come in many forms, under most legal systems all are underpinned by explicit contracts.[2] The advent of DLTs and smart contracts allows firms to embed financial contracts in technological products, where the financial component is operationalized by a cryptographic protocol. This is a step beyond simply replacing a currency as a unit of exchange and inter-temporal transfer of value, but actually replaces the need for a legal medium to act as an enforcement mechanism for commercial contracts.

We summarize our arguments on cryptographically enabled contracts via distributed ledgers and block chains as follows:

1. **Combinatorial and modular** – unrestricted smart contracts are potentially 'Turing Complete', (or 'Computationally universal' that is simple modules can be combined to replicate algorithms of arbitrary complexity). Hence, a series of smart contracts can replicate any essential components needed to initiate an organization and appropriately redistribute property rights.
2. **Disruptive** – DLTs and smart contracts provide opportunities and solutions to current requirements and creates opportunities to create entirely new requirements and entities. For example, the ability to add financial value to electronically mediated transactions without recourse to a currency backed by either a legal mechanism or a physical commodity (such as gold) managed by a central counter-party means that the concept of a financial intermediary is transformed into an algorithm which simply requires some form of execution.
3. **Unruly** — the very same Turing-completeness implies it is not possible to determine in advance and possibly in some automatic way whether a smart contract would have some desired properties[3]) and hence:
   (a) in the general case *only the execution itself would determine what a contract outcome would be* and the agreement between the counter-parties to continue to work on the actual

[2] Some countries, North Korea and Belarus are key examples, do allow domestic firms to write explicit individual contracts, but manage all organizations through some centralized principles that amount to the same form.
[3] Rice's theorem (Sipser 2012, Proof 5.28, pp. 243) states that no recursive program can take a non-trivial set of general programs (e.g. all versions of smart contracts populating a distributed ledger with an expressive programming language such as in Ethereum) and discriminate the subset of programs satisfying a non-trivial property (e.g. the contracts guaranteeing an always or eventually positive return on investment).

ledger directly replaces the enforceability medium provided by a social planner to enable the nexus of contracts that form firms.

(b) as the contract execution is distributed to all entities of the DLTs the notion that a firm as a static representation of a nexus of contracts with persistent property rights becomes less important given the ability to recombine a new firm *without costs but also without the certainty to hold on to assets or be accountable for liabilities*.

The radical, unruly nature of this innovation is well captured by the Ethereum Classic's manifesto:

By entering into contracts on Ethereum Classic, you can be certain that the network remains neutral. The outcome of transactions will be dictated by code you voluntarily interact with. Unless explicitly defined by the contract code, there are no reversals, no undos, no opt-outs. Transactions are final; applications are unstoppable.

We will show that the arguments above are: a) fundamentally disruptive to the current notions of how firms are formed and the meaning of destruction and recombination in this context; b) the types of recombination and disruption envisaged are real and that we are beginning to see examples of ad-hoc firms appearing. Finally, we discuss, in some detail, examples of resistance and place some social welfare context on this innovation.

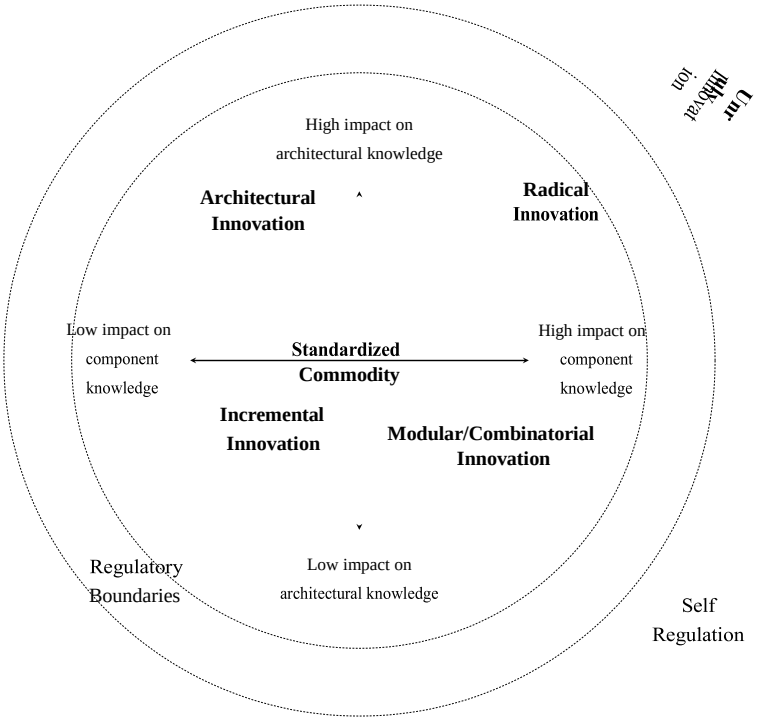
2. Theory on Disruptive Technologies

To discuss the innovation impact of DLTs and smart contracts it is useful to map the key interest groups and actors behind new and old *payment transactions networks* (PTNs for short) into the classical terminology from Alford (1977). Each PTN is characterized by a governance structure that places the actors within the PTN cohort in the position of "professional monopolists" in this financial system (Alford 1977, ch:xiv). In short, this position permits control over the "strategically structured interest" in relation to the resources and power dynamics of those leading financial systems (ibid.). Simply put, there exists "a continuing struggle between major structural interests operating within the context of a market society" although first applied to the health care context, this concept can be readily applied to the PTN system (ibid.). On one side, the "professional monopolists" control the PTN resources whilst the "corporate rationalizers" challenge their power (i.e. new entrants, lobbyists

and technological innovation), and finally the community population seek improved financial transactions (ibid.).

The new developments have seen the introduction of cryptocurrencies such as Bitcoin, Ripple and centralized ledgers (for a non-technical survey see (Massacci et al. 2016, § 3-6)). Some of these proposals, e.g. Danezis and Meiklejohn (2015), offer only minimal innovation and maintain the monopolist status quo in the financial sector. Other proposals have the capacity to be disruptive to the order within the financial sector, displacing the need for controlled PTN and creating an autonomous, self-organizing alternative that would be governed by and serve the community population. To examine the level of potential disruption to the financial industry posed by innovation and technologies our discussion will explore the innovation literature. In addition, we shape our

Figure 1 (De)Regulation and Innovation Matrix



Note. Adapted from Henderson and Clark (1990).

discussion looking at the interaction of disruptive technologies and combinatorial innovations and modularity to emphasize the super modularity surrounding DLTs, smart contracts and the resultant impact on structured interests.

2.1. Disruptive Innovation

Prior to the introduction of the term 'disruptive innovation' (Christensen and Snyder 1997), there were forerunning ideas such as Schumpeter (1942) creative destruction, a theory heavily influenced by Marxian destructive forces theory linked to the concept of the owners of production dictating innovation and change (i.e., professional monopolizers). In the 1980's we progressed to Henderson and Clark (1990) model of radical innovation (see Figure 1 above). Here, the authors explain the difference between incremental to radical innovations linked to how the knowledge component of an innovation impacts on the existing (architectural) levels of knowledge.

What we can observe from Figure 1 above, is that the definition of 'unruly' innovation is hard to comprehensively describe, i.e. how does this differ from radical? Clarification is required in terms of developments in this field since the 1990's, more specifically Christensen and Snyder (1997) The Innovator's Dilemma cemented the term 'disruptive innovation' which became synonymous with his name. Yet, to date there is much debate in the literature regarding the definition and differences between disruptive technology and disruptive innovation (Danneels 2004, Markides 2006). As we will argue in the rest of the paper, unruly innovation moves innovation outside the broad rules of the market that even 'radical innovation' do not completely break.

We start our review by illustrating Christensen's perspective. Christensen and Snyder (1997) postulated that when individuals or a firm embark on a new innovation irrespective of the target market, the route is uncertain and can be viewed as a journey into the unknown, a non-linear path gradually progressing from chaos to order. Hence, the introduction of a disruptive technology or disruptive innovation is a change that helps create a new market and value network, and eventually goes on to disrupt existing networks in an unanticipated (chaotic and complex) manner. Although, Christensen introduced the term 'disruptive innovation' he argued that this was a more comprehensive terms as he espoused that technologies in themselves are rarely intrinsically disruptive; rather, when technology is linked to an organization's business model, it is the latter

model that enables the disruptive impact in creating a new organization order i.e., unit.

Linked to the above debate, in examining the broader literature the terms disruptive technology and innovation are widely cited interchangeably in the business and technology literature to capture innovations that emerge into a market or industry and invoke change (Yu and Hang 2010). One of the key findings of Christensen's work is that disruptive technological innovations eventually grow to dominate the market (i.e., Apple's ascent over Nokia). Christensen and Raynor (2003a, p.70) make this point forcefully by arguing that *"disruption is a process and not an event, it might take decades for the forces to work their way through an industry but [they] are always at work."* Similarly, Danneels (2004, p.247) summarised existing theory on disruptive innovation by pointing out that *"disruptive technologies tend to be associated with the replacement of incumbents by entrants."* If correct, such a fact carries serious implications for incumbent firms that a firm's only option is to accept the disruption and proceed to exploiting the opportunity it presents. Christensen and Raynor (2003) suggested that established companies could exploit a disruption only by creating a separate unit. If we apply the arguments reviewed thus far to DLTs, we can see how DLTs redefine the concept of a firm as the innovation nexus, as Christensen argues relative to the firm's business model driving innovation and creating units. Rather through cryptographic protocols, a nexus of financial contracts are embedded in technological products, this disrupts both the market and value network created (according to Christensen) and the current dominant actors in the financial system (i.e., removing the monopolists legal control).

Turning to reviewing mainstream technological innovation studies there is clear demarcation between two types, with the caveat of adopting different terminologies for different stages in history. Simply put, i) revolutionary, discontinuous, breakthrough, radical, emergent or step function technologies and ii) evolutionary, continuous or incremental technologies (Florida and Kenney 1990); (Morone 1993); (Christensen et al. 1998). If we refer back to Henderson and Clark (1990) modular vs architectural innovation model (see Figure 1 above) the authors were able to move beyond these two categories and explore the causes of failure in firms as the result of core technological innovations companies with strong competences in component technologies might ignore the competitive implications of the architecture changes. Hence, the architectural innovation theory made the contribution of explaining competency-enhancing or destroying theory was not

accounted for in the literature at that stage.

Likewise, Punctuated Equilibrium Theory (PET) is also useful in expanding the above categories to understand disruptive technological and innovation effects on firm's operating systems. PET has three major components, which are: (i) deep structure, (ii) equilibrium periods, and (iii) revolutionary periods (Gersick 1991). Deep structure is the set of fundamental "choices a system has made of (1) the basic parts into which its units will be organised and (2) the basic activity pattern that will maintain its existence" (Gersick 1991, p.14). The deep structure can be seen as the basic design or architecture of the firm and during equilibrium periods this basic design or architecture of the firm remains the same, consisting of maintaining and carrying out the choices represented in this basic design (i.e., sustaining according to Christensen). During this period, innovation is incremental in nature, to compensate for internal and external fluctuations without affecting the deep structure (i.e., 'business as usual'). Gersick (1991) also notes that the pursuit of deep structure choices may result in behaviour that is turbulent on the surface. Hence, the deep structure generates strong inertia that prevents the generation of alternative deep structures, or disruptive innovation to fundamentally change the firm.

2.2. DLTs Disruptive Innovation in the Context of the Firm

In the firm context, the process of the introduction of DLTs can be interpreted as follows. The deep structure of the firm refers the firm's core, which according to McKinsey's 7S model, is the firm's culture (i.e., shared values). This interpretation is shared by Hannan and Freeman (1984), who argue that the most important element of the firm is its mission, which is culturally determined and a shared value (or raison d'etre) of the firm. During the equilibrium period, the elements of the firm converge around its mission or core, the firm's strategy, structure, staff, systems, skills, style, and stakeholders. At this stage, all the elements (components) of the firm's configuration become more tightly coupled and increase efficiency. Yet, a side-effect of this process is reduced effectiveness as the organisation becomes more and more inert (i.e., inflexible). At a certain point, the organisation is no longer able to adapt to its changing environment, the introduction of disruptive technology such as DLTs. Misalignment ensues, increasing firm tension, conflict, resistance and stress. The crisis emerges where the deep structure needs to be dismantled (voluntarily or forcefully) in order to adapt or self-organise to the new requirements driven by environmental pressure, if the firm wishes to survive (i.e., a short revolutionary period). DLTs present this

pressure by fundamentally restructuring financial contracts, use of cryptocurrencies and can be used to create Decentralised Autonomous Organizations. In Figure 2 we outline the current proposals for using DLTs in financial services. Here we see a centrally banked RTGS system supplying legal tender that is exchanged for ledger tokens. These ledger tokens are applied to a number of areas. In red there is a DAO, which

Figure 2 A Collection of DAOs Operating on a DLT platform.

Note. The black lines in the background represent connections between ledgers. Red and blue represent the most complex smart contracts. Green and orange the simplest. Components can migrate and attach themselves to the ledger then detach and discontinue for negligible cost in both directions.

replicates the financial contract side of a regular firm. In green is a pure cryptocurrency like Bitcoin that can act as a store of value, by exchanging centrally banked money for computational effort. In dark blue we outline three different types of capital market, first a continuous double auction for standardized securities (like stock market), an over-the-counter market for non-standardized assets (housing, debentures) and a venture capitalist market for supplying entrepreneurs. In each case the DLT acts as a means of ensuring that transactions have the integrity and permanence required for standard activities.

Returning to Christensen, his theory received some support while proposing their own slightly different

views. For example, Adner (2002) identified that a critical reason for the switch of consumer choices from sustaining to disruptive innovation was the decreasing marginal utility from the performance improvements in major dimensions, in addition to the new value propositions and affordable prices discussed by Christensen. Meanwhile, others criticised the vagueness of the concept of disruptive innovation. Danneels (2004), (see above) suggested that several authors seemed to think that Christensen did not provide a precise and consistent definition of the term disruptive technology. Tellis (2006) challenged that it would be very difficult to differentiate underperforming technologies from a technology with inferior performance but finally ending up being disruptive.

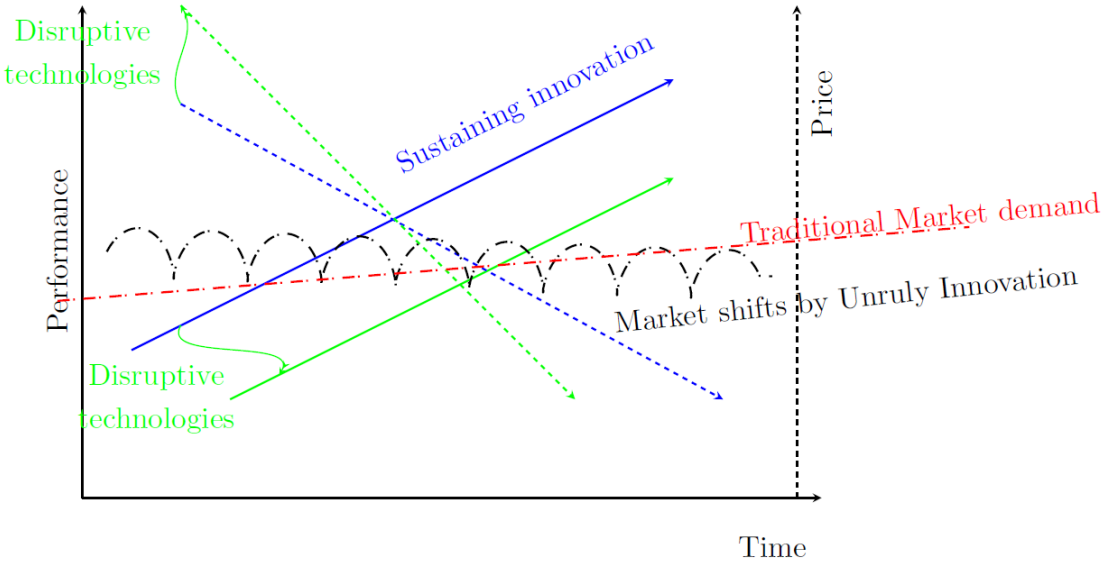
Govindarajan and Kopalle (2006) contribution introduces an innovation measure to include high-end as well as low-end disruptions, provides a more general view of disruptiveness of innovations and explores beyond the case of low price/low performance. Disruptive innovation (having inferior performance in traditional attributes) with a high price, which Govindarjan and Kopalle referred to as high end, is not explored within Christensen's theory. In Figure 3 below, the authors use cellular phones to exemplify the above theoretical issue to highlight the trade-off between relatively high priced goods versus convenience and portability (e.g., iPhones retail at USD600-800 per unit). Over time, cellular technology improved in providing reliable coverage at a reasonable cost to satisfy consumer demand, causing the disruption. According to this study, a disruptive innovation should (i) be inferior on the attributes that mainstream customers value; (ii) offer new value propositions to attract a new customer segment or the more price sensitive mainstream market; (iii) be sold at a lower price; and (iv) penetrate the market from niche to mainstream, still placing the firm as the innovation nexus (Yu and Hang 2010).

2.3. Unruly Innovation as Disruption of the Rules of the Market

To support our argument that DLTs go beyond the firm as the nexus of innovation it is necessary to define innovation in the literature by way of illustrating the difference DLTs pose. Sustaining innovation is a journey that creates better products at a higher premium to attractive customers.

According to Christensen and Snyder (1997), incumbents tend to prevail in such circumstances. Disruptive innovation is oriented towards commercialising a simpler or more convenient product, aimed at new or unattractive customer sets for a lower premium (see below, cellular phone innovation). This would favor new market entrants beating the incumbents. In short, there are several

Figure 3 Product-wise innovation



Note. This concept is extended from Govindarajan and Kopalle (2006): sustaining innovation moves in time along a given performance trajectory, for example by improving the performance of a product in time (blue solid line), or by reducing its price (dotted line). Disruptive innovation create new performance paths (green solid line) or new price curves (dotted green lines) that are in alternative to existing products. However neither of them substantially changes the market demand. Unruly innovation can also change the market behavior as a whole, and thus generate a shifting market demand (coiled line).

business examples where the dominant companies suffer from a flux of such products, start-ups attack established competitors, they disrupt them the caveat being that not all innovation stems from start-ups.

The first aspect of the model illustrates the customers' ability to utilise improvement as a single line. Yet, Christensen acknowledged that in reality, customers are distributed around the median shown. Hence, there are many such lines, or tiers in a market that customers will occupy illustrated by the distribution curve (right). Interpreting the model, this complies to management practice of managing stakeholders expectations whereas, the introduction of DLTs proposed in this study changes the customer role such that customers can define financial contracts within technology and self-organise. One consideration from this model is that in introducing new technology for PTNs, customers' ability to utilise the DLTs and options such as Bitcoin is taken into account for disruption to occur in the current financial system.

A significant difference in the introduction of DLTs as a disruptive innovation is that contrary to Christensen and Snyder (1997) distinction between sustaining and disruptive innovation, targeting the different customer tiers, the appeal would be universal. Not only would there be a trade-off in terms of other benefits, typically innovations are simpler to use, more convenient and usually less

expensive (i.e., removal of transaction charges applied by banks), this model does not account for the modularity aspect of DLTs, decoupling and dismantling the old order and creating sub-systems of systems (i.e., payment options outside of firms as the innovation nexus).

In particular, DLTs differ from the current disruptive innovation literature regards the concept of modularity or the intentional decoupling of interoperating systems-systems of a larger system (Tiwana 2008: 769-70). Linked to our previous discussion of decoupling and PET, the notion of modularity adopts a complex systems approach in that the system is more than a sum of its constituent parts and can adapt to working interdependently or independently with the ability to combine or re- combine in a self-organising manner to support the 'whole' (Karim 2006). In the business context, this can be witnessed in interfirm partnerships and collaboration. What DLTs offer is we contend 'supermodularity' by creating decoupled autonomous subsystems that connect to a larger system defined and created outside the existing financial system structure. This establishes a different interoperating model facilitating communication, exchange of payment and functionality for the community of users.

Christensen and Raynor (2003b, p.39) espoused that a key question for disruptive innovation:

"it is a story of rational managers facing the innovator's dilemma: Should we invest to protect the least profitable end of our business, so that we can retain our least loyal, most price-sensitive customers? Or should we invest to strengthen our position in the most profitable tiers of our business, with customers who reward us with premium prices for better products?"

The authors continued to examine (part of our discussion in this paper) the potential for Internet Banking and subsequent technological development, interestingly at that time it was argued that disruption using this technology was not perceived as possible (Christensen and Raynor 2003b). The rationale behind this claim included several reasons; i) an insufficient large population who have the skill or money to open an account and, ii) banks penetration level is high which rules out new-market disruption for Internet banking. However, as we have shown the issue raised around innovation in this arena is the notion that through supermodularity a range of diverse customers can remove the need for bank account privileges and features at a low service price in adopting DLTs (i.e., no fees or need to move banking provider). Hence, disruption as a theory, a "conceptual model of cause and effect that makes it possible to better predict the outcomes of competitive battles in different

circumstances" is challenged by DLTs innovation as there are a plethora of asymmetrical levels of motivation users and economic implications from the decoupling of the current system and creating multiple combinatory subsystems revolving around the movement and payment of money (ibid, p.40).

This extension of modular innovation models for DLTs to supermodularity will require new knowledge for one or more components whilst the architectural knowledge necessarily has to change (i.e., the financial system). As industries have evolved the buyer-supplier relationships have progressed to increasingly modular products leading to shifts towards agile and disaggregated supply chains (Langlois and Robertson 1992, Zenger and Hesterly 1997, Schilling and Steensma 2001). Innovation is the modular sense has witnessed low modularity products being tailored to meet customer expectations of a product which can necessitate an upskill effect in the customer's product to match the component(s) technological development (self-organizing system). Examining highly modular components as provided in DLTs enables components to be incorporated into multiple end products (e.g., embedding financial contracts, etc.) with little impact on the component or end-product in allowing the transfer of monies (Ducy et al. 2000). Indeed, viewed from this perspective, supermodularity creates supply chain flexibility in the financial industry by reducing the need for interfaces between the banking system, community in receipt and component suppliers (Sanchez and Mahoney 1996). In short, the opportunity presented in adopting different DLTs and PTNs raises the issue of changing the models of disruptive innovation and decoupling the power and governance currently embedded by the professional monopolisers in the current financial PTNs towards a more emergent and self-organising subsystem of payment transfer.

Table 1 Disruptive criteria sheet for DLTs (entrant)

Phase	Criterion	Evaluation
Foothold market entry	Products perform worse based on established attributes	**Fulfilled**: Low transaction throughput and financial services as well as supports are limited.
	Products are cheaper, simpler, more comfortable or more reliable	**Fulfilled**: Easy to deploy and scale, better user privacy, higher fault-tolerance.
	Products address current non-consumers	**Fulfilled**: Customers who want better privacy will seek to use DLTs.
	Profitable business model targeting over-satisfied customers	**Unknown**
	Investors allow experimentation	**Fulfilled**: Many projects funded and launched: HyperLedger, Ripple, Ethereum. Bank of England calls for centrally-banked cryptocurrency (RSCoin).
Main market entry	Products are based on standard components	**Fulfilled**: Well studied components are used such as cryptography, distributed system, and digital time-stamping.
	Strategic resources (licenses, capital, etc.) are accessible	**Fulfilled**: Mostly open source software and cheap hardware.
	Network for PDI is expected to be large	**Fulfilled**: Widely deployed communication network (the Internet).
	PDI is compatible with existing network	**Unfulfilled**: Only some credit-backing cryptocurrencies such as RSCoin or Ripple are backward compatible with central bank currency.
Failure of incumbent	Business model is significantly different	**Fulfilled**: Central Authority is removed.
	Processes are significantly different	**Fulfilled**: Peers work together to keep record of the ledgers.
	Value network has a low overlap	**Unfulfilled:** there are central bank currency that back cryptocurrencies such as RSCoin or Ripple.

DLTs with smart contracts evaluated against phases and criteria from Govindarajan and Kopalle (2006).

DLTs, even at a cursory glance, fit the model of a disruptive innovation. Table 1 above, reviews the features of a DLT from Govindarajan and Kopalle (2006) viewpoints of foothold, main market dominance and failure to the incumbent to illustrate such potentiality.

2.4. Framing FinTechs DLTs as Actors in Financial Markets

Financial markets are inextricably linked to the social where economic actors (i.e. investors, traders, institutions and so on) can impact governments and national economies (see Cetina and Preda (2007) for a sociological history of financial markets). Claiming that DLTs and smart-contract could yield to self-organisation of financial markets and systems seems at odd with the normally intended notion of economic actor. This definition has been widely debated (See for example Callon (1998) vs Miller (2002)). A consensus has emerged that actors are not "made up of human bodies[. . .] technical devices, algorithms" Callon and Muniesa (2005, p.1230): 'agencement' or sociotechnical combinations. Hence our claim is that the deployment of smart contracts on a DAO is just such extension: once contracts are automatically executed they become actors. Cetina and Preda (2007, p.126) move the agencement debate forward in exploring how architectural changes (See Figure 1) have occurred so that a market "is stable only long enough to enable transactions to occur and changes with transactions." However at the time of writing, no method of a "superordinate mechanism that reflects all the information in a network and makes it available simultaneously to all concerned" existed (ibid.). DLTs and DAO constitute the essential game changer that allows to move FinTech innovation from architectural to radical and eventually to unruly (See again Figure 1). Indeed, DLTs have the potential to be what (MacKenzie 2008: 13) termed "effective" or "Barnesian" performativity (the actual realization of the market is much closer to the economic theory that describes it). A topical example is the authentic distributed nature of a DLTs implementing a financial market (Massacci et al. 2017a) as described in the theory Spulber (1996) as opposed to the actual implementation which requires the mediation of the Exchange Harris (2003). At the same time they have features that makes their nature counter performative (less likely to adhere to the process descripted by the theory) such as the finality of code execution: there cannot be a legal interpretation as code is law (Lessig 1999) Our key

observation borrowed from MacKenzie (2008) is that the properties of artefacts, technological systems, are not 'details' that FinTech analyses could set aside, as those technological aspects may be such that new and alternative forms of organization become possible.

3. Disruption by changing the FinTech game

The classic paradigm suggests that a disruptive technology is something that does something that dominates all incumbents in several dimensions. Indeed, this sits within a classic economic paradigm of substitutable goods, if a form of consumption can be provided more cheaply or be fully dominated by a good that offers far more dimensions to consumption within a similar cost frame then it is disruptive, with Nokia versus Apple a typically cited example.

Table 2 Conceptual Differences Between Types of Innovation

Context	Incremental	Disruptive	Radical	Game Changer
Components	Streamline and simplification	Cheaper possibly compatible	New capability on existing framing	New framework, no backward compatibility
Modularity	Bespoke to plug-in within existing frameworks	Combinatorial	Extending the current configuration	Combinatorial, but not with previous modules
Competition	Standardized substitutes	Monopoly	Limited	Monopoly
Regulation	Mature	Unknown	Within norms	None
Fixed Costs	Low	Unknown	High	None
Cultural	Overlooked	Immediate	Overlooked	Invasive
Consumption	Same as before	Extended	Extended	New
Resistance	Low	High	Low	Intended, but difficult

However, we introduce a new form of disruption which we call 'changing the game'. This is not about adding features (dimensions) to the consumption of a good, or providing an equivalent consumption at a cheaper price, it is simply a wiping of the board that re-shapes the entire FinTech spectrum.

These issues are also found in the standard critique of the classic Prisoner's Dilemma problem. Binmore (2007) notes that many commentators on Merrill Flood, Melvin Dresher and Albert W. Tucker's original thought experiment vehemently disliked the no-cooperation solution. However, all explanations for why 'their' formulations of the Prisoner's Dilemma with a cooperative solution is an acceptable one amount to the same thing: the game is changed. For instance, the players "knowing" that the other will not defect, or that there was utility to be gained for acting altruistically. Simply, the landscape of the entire economic interaction is changed to reveal an alternative solution.

When a technology changes the landscape of economic activity, it is essentially changing the

parameters of the game. Very few technologies can claim this feature and most that do are a nexus of classical disruptive innovation and combinatorial innovation. For instance, the introduction of interchangeable machined parts allowed mechanization to enter every aspect of the production and consumption cycle that underpinned the industrial revolution.

Table 2 above presents a conceptual dichotomy of changing the game in comparison to incremental, disruptive and radical innovation.

3.1. Resistance and changing the game?

We suggest that the reason a new mode of innovation needs to be delineated is a function of the variation in fixed costs, cultural impact, variation in consumption and the ability to resist, both by society and incumbents. In reverse order, when a new potentially disruptive technology is innovated, resistance by incumbents is to be expected. However, the benefit to society may be such (indeed is the norm) that social planner mechanisms are not enacted to mitigate the disruption. In certain cases, and we will illustrate some of them in our next context, it might be desirable to hobble the innovation through the actions of a social planner to reduce or eliminate the disruption on incumbents. Three recent innovations, IR tagging of freight to improve electronically managed supply chains, algorithmic analysis of individual consumption patterns by retailers and high frequency trading are examples where social planners have enacted mechanisms to deliberately reduce the effectiveness of the technology to meet the requirements of society, see for instance Securities and Exchange Commission (2014). A changing of the game, is a case whereby a social planner cannot prevent the innovation from reshaping the economic landscape.

What is the mechanism that prevents regulatory action? We posit three domains that need to converge for this to occur. First consumption. The innovation must provide a new mechanism for consumption that differs from existing consumption paradigms. For instance, certain cryptocurrencies permit the exchange of value without any centrally banked oversight, hence the economy supported by these transactions is essentially dark to the rest of the regulated economy, where money has some traceability. Whilst a black economy obviously existed before DLT enabled cryptocurrencies, the medium of exchange was still via centrally banked money, hence the problem was information processing by enforcement and not existential, cryptographically enabled transactions of the correct type cannot be tracked and their existence in law is debatable, it is essentially a recorded agreement between individuals that is carefully ledgered.

Culturally, changing the game technologies are invasive. That is the recognition that they are being used is normally overlooked and the cultural landscape changes in a way that is gradual, but essentially irreversible. For instance, children begin to use money ledgered in interconnected games to substitute for real transactional exchanges. This is a centralized ledger, but a distributed one could be provided for essentially no cost and the very act of migration gradually destroys the previous economic paradigm. More pertinently, if a firm provides a mechanism for real time gross cash settlement that can be exchanged externally for centrally banked money, but only requires a modicum of commitment to providing computational capacity to record their ledgers (for instance on connection per transaction), then firms will gradually migrate to this platform and eventually kill the incumbents (monolithic PTNs). This leads us to the final element, fixed costs. When a technological innovation has fixed and abatement costs close to zero the diffusion to the technology has no financial obstacles.

Most firms already either have in house, or buy in substantial computing power, some of which is unused. Simple implementation of the protocols for DLTs allows the firm to flexibly choose when to conduct a transaction and/or axiomatize contractual structures within the firm. Furthermore, unlike radical innovation with a high impact on component and architectural knowledge, a changing of the game is a mechanism of 'normalizing' complex process into simple ones, that can be viewed as easily conducted by the individual or individual organization. For instance, the process of conducting financial transactions could be viewed as a high knowledge, high fixed cost problem that is best dealt with by specialist intermediaries. Similarly, the mechanism of conceiving an organization as a nexus of contracts requires a highly structured set of legal mechanisms that interact with a social planners laws to allow the concrete creation of the firm as an entity. Modular smart contracts 'normalize' this mechanism such that the creation, running and dissolution of a firm is a costless sequence that is anticipated to be transitory, than presumed to be persistent.

4. The Rise of the DAO and Inevitable Risks

A DAOs is simply a cryptographically enabled nexus of contracts that codifies an entity that is autonomous, in the sense of the legal framework is cryptographically codified. In Table A in the appendix we outline some core components of a transaction mechanism involved in a cryptographically enabled PTN. As previously noted once an electronic action has a 'real' financial

value attached to it then much more complex contractual arrangements can be enabled and codified.

Bitcoin, https://bitcoin.org, is the first and most successful payment DAO. Furthermore, several simple extensions of a payment DAO can also be directly implemented in Bitcoin using its (non-Turing-complete) scripting language. Bitcoin script supports variable and constant declarations, basic arithmetic operations, and evaluations of hash and signature as well as two time constraint operators. As such, simple applications such as external financial data source, crowdfunding, escrow, intermediated payment, fair lotteries, etc. are possible with Bitcoin scripts (Atzei et al. 2018). Similarly, Stellar, https://www.stellar.org, is a payment DAO but it additionally features *multisignature* that requires multiple signers, and allows the creation of more complex smart contracts. However, it is only until the launch of Ethereum, https://www.ethereum.org that smart contracts can be fully developed using a Turing-complete language.

Since the launch of Ethereum in 2013, we have witnessed many other similar smart contract platforms for DAO. The noticeable new platforms are listed in Table 3. Just to highlight a few among them: (1) NEO, https://neo.org, which is also dubbed the Chinese Ethereum[4], reaches 1000 transactions/second (TPS) while Ethereum is still struggling with scalability issue[5]; (2) STRAT, https://stratisplatform.com, a "Blockchain as a Service" platform that is tailor made for enterprises to create their own custom decentralized applications; and (3) EOS, https://eos.io, which focuses on providing toolboxes for decentralized applications development such as shared databases, authentication systems, account recovery, cloud storage and hosting, scaling, all paid with EOS tokens.

[4] NEX, https://neonexchange.org/, is featured as an effi cient decentralized exchange while RedPulse, https://www.redpulse.com, is considered the "next generation intelligence and content ecosystem for China markets".

[5] Ethereum has plan to shift from the heavy Proof-of-Work mechanism to the lightweight Proof-of-Stake mechanism but this is still under development.

Table 3 Noticeable alternative DAO platforms in comparisons with Ethereum.

Platform	URL	Enhanced Features
NEO	https://neo.org/	offers high throughput (1000 TPS)
STRAT design for	https://stratisplatform.com/	offers "Blockchain as a Service", specially private and custom enterprise DAOs
EOS	https://eos.io/	offers extended toolboxes for decentralized applica- tions development
LISK	https://lisk.io/	allows side chains alongside with a main chain for independent transactions processing
WAVES provides a	https://wavesplatform.com/	allows multiple tokens development and seamless tokens exchange mechanism
Chainlink contracts	https://www.smartcontract.com/link	offers external data sources for smart

4.1. Case Study: Ethereum and the implications of codification

The first DAO and the platform on which it was built provides a useful example of the dangers associated with such entities. Ethereum is a scripting language (the platform) that runs off a core engine called the Ethereum Virtual Machine, this is the scaleable distributed infrastructure that allows the contracts written in the scripting language to be executed. Unlike Bitcoin and other cryptocurrencies Ethereum is built from scratch in terms of contracts, that trade tokens (called) ether transactions on which are stored on a distributed ledger run on the hardware provided by the participants in the project. Ethereum was started in 2013, by cryptographers and has market capitalization of $1 billion as of December 2016. The path of Ethereum is naturally uncertain as one of the key features of a platform is that unwinding it should be as natural as creating it, given the low frictions for both actions.

Key points, to join an Ethereum DAO you simply need to implement the protocol, demonstrate some proof of effort or exchange centrally banked money, then proceed to write smart contracts that 'do' certain things, such as distributing money contingent on some external input. This could be a contingent claim, like a financial derivative, or in response to some form of effort, such as building some software or some other tangible activity that can be verified cryptographically. An example could be that a truck driver delivering some goods takes a photograph of the stars or some geographical landmark then the pictures are 'hashed' so that a complex algorithm is solved (this algorithm should be time dependent) with an easily verifiable solution. So the proposer has to expend computational effort to prove their 'state'. The smart contract in the DAO then rebalances the ledger to reflect this state and its implications for other agents in the ledger. So in the truck driver case the

verification releases a payment that the driver can exchange for centrally banked money or keep in the DAO for storage.

The contracts build in Ethereum can be 'very' smart, indeed, a key claim of the scripting language is that it is Turing complete. A Turing complete programming language sits at the very top of the complexity scale. That is for any non-trivial algorithm there is no automatic mechanism that can check all of the possible outcomes of an algorithm that it designed in that language. Hence, a clever programmer can effectively design any type of organization that can be imagined, as in this case the language is in the form of codified clauses within contracts.

On the practical usage of Ethereum smart contracts, (Bartoletti and Pompianu 2017) demonstrates that they have been used for various application categories: (1) financial applications, which is the original intention; (2) notary, in which the smart contract is used to persist data like photos, music, messages, etc.; (3) games of chance (Dice, Roulette, RockPaperScissor) and some other simple games based on skill (Etherization, PRNG challenge); (4) wallets which specialize in managing keys, signatures, transactions; and (5) advanced programming libraries for smart contract development, e.g. math, string processing, etc.

The codification of laws is a popular conceit in the legal literature, with foundational contributions from Lessig (1999, 2009), Perritt (2000) that warn of the implications of legal mechanisms enshrined in computer code. A key component of our legal infrastructure is Tort or Delict recourse within a civil framework. When a contract is disputed the counter-parties to the contract dispute their case to some impartial adjudicator who acts with the authority of society to 'fairly' resolve disputes, interpreting the clause structure of the contract. The adjudicator then has the authority to place economic and physical sanction on an individual or entity if the adjudicator's proposed remediation is not enforced. Whilst this obviously can happen in our real world setting, in a codified system there is no method of enacting remediation than that which the original algorithm intended. Hence, when building a DAO safety is most certainly not guaranteed, indeed to replicate the complexity of normal organizations, this feature is a necessity.

Indeed, a recent survey on the security of Ethereum smart contracts (Atzei et al. 2017: 21) has pointed out that "the difficulty of detecting mismatches between their intended behaviour and the actual one" has been the main cause of smart contract vulnerabilities. The authors suggested that non-Turing complete and human-readable languages are preferable for specific domain applications

as “the choice of using a Turing-complete language limits the possibility of verification” (ibid: 21). A comprehensive list of discovered smart contract vulnerabilities such as variables type cast, ether lost in transfer, etc. can be found in the aforementioned survey (ibid.). Furthermore, DAO vulnerabilities cannot be treated as “normal” security vulnerabilities. As it is shown in (Massacci et al. 2017b), security and economics are one for DAOs: the failure of a security property, e.g. anonymity, can destroy a DAO because economic attacks can be tailgated to security attacks and there is no possible technical fix for the DAO as we will see in the following discussion.

An organization called ‘The DAO’, which was one of the first DAOs built in a smart contract enabled DLT. At a peak the value of ‘The DAO’ was about $100 million, stored entirely in Ethereum currency units. The objective of the DAO was to create a venture capitalist fund designed to initiate other projects and demonstrate the creation of DAOs, see daohub.org.

As noted, distributed ledges are specifically designed to make it impossible for individual parties (or even a large set thereof) to tamper the sequence of transactions recorded in the ledger. However, an unknown individual, exploited the Turing completeness of the contract to construct a routing of transactions in the ledger that allowed that individual to take control of a large proportion of the invested capital (resulting in a final loss of about $3.8 million, see https://forum.daohub.org/t/scam-and-suspicious-project-list/6757). The transactions were legitimate, in the sense that they were allowable under the initial coding of the DAO. However, the money was not used in the real world for the venture capitalist objectives envisioned by the creators of the organization.

Hence, in the attempt to reverse the DAO financial crisis, Ethereum designers proposed a solution outside the protocol itself: encourage parties to upgrade to a protocol client version that makes it impossible for the “hacker” to monetize the solution. This solution illustrate the true role that the Ethereum authors have in the game and that they have naively (or deliberately) downplayed: “Code is a regulator in cyberspace because it defines the terms upon which cyberspace is offered. And those who set those terms increasingly recognize the code as a means to achieving the behaviours that benefit them best.”

The attempts to fix the ‘The DAO’ proved difficult as to rewrite the central nexus of contracts forming the organization requires the majority of members to agree and this level of cooperation proved elusive. Indeed, a large fraction of the members of the Ethereum Community refused to join

the new redressed ledgers, issued a Declaration of Independence[6] and continued to maintain the "classic" ledger:

Let it be known to the entire world that on July 20th, 2016, at block 1,920,000, we as a community of sovereign individuals stood united by a common vision to continue the original Ethereum blockchain that is truly free from censorship, fraud or third party interference.

Outside of the inherent instability of the 'The DAO' several further implications of its existence were stark. First, the organization was inherently stateless. Given the structure of contracts generating the DAO no state could reconstruct the ledger and hence could not identified payments or receipts between members for tax purposes or any other. This falls into the third point of danger in the Lessig (2009) classification, that entirely codified economic activity is inherently separate from the redistributive component of a firm's economic interaction with society.

'The DAO' was assembled in an ad-hoc fashion, investment in the venture capital projects agglomerated to 'The DAO' by simply implementing the protocol built in Ethereum and then exchanging the appropriate capital. The nexus of contracts then processed further payments and receipts from the venture capital component and redistributed them accordingly. The speed of the failure in the 'The DAO' does illustrate the risk of crashes.

5. A Geometric Interpretation Risk from Unruly Innovation

The nature of innovation and the value and risks associated have been widely studied in the past using simple stochastic process to illustrate, geometrically, the nature of the risk vector. Levinthal (1991), Swaminathan (1996), Gimeno et al. (1997) and Denrell (2004) utilize a combination of random walks and martingale models of bets on future value to understand firm mortality within a stochastic framework. In our case we can model both the opportunity structure and the risk structure inherent to designing DAO within Turing complete frameworks, a modelling approach more akin to that suggested in Coad et al. (2013), for innovation and DeTienne et al. (2008) for risk bearing. To better understand the general nature of the risk and the dire fact that it is not eliminable we consider natural model of evolution of the market. Assume that an agent valuation of a DAO with M participants can be captured with a N-dimensional vector $\boldsymbol{x(t,M)}$ of 'component evaluations' of the

[6] Available at https://ethereumclassic.github.io/assets/ETC_Declaration_of_Independence.pdf.

DAO in the positive real space $R^+x\ N \rightarrow R^N$ which captures the evolution of the DAO in time and in the number of participants. In a financial market this could be the valuation of a particular asset through clearing the supply and demand of securities (For example see Massacci et al. (2017a) for distributed ledger implementation of a Futures Exchange). In a social network this could be total activity, number of adverts consumed and total trades.

Our main assumptions are that the value of a DAO is built into the business model. Organizations can be constructed in an ad-hoc way with a specific set of objectives and assign ownership to digital assets in a manner similar to a nexus of contracts operating within a standard jurisdictional legal framework. However, we will then model the components of such a set of contracts as being designed to be Turing complete with dynamic updates. This offers a flexible mechanism for designing, combinatorially, new components and hence facilitating potentially disruptive innovation, but also has risk associated with unintended and potentially harmful execution, which proffers systemic risks to the organization, that destroy the DAOs asset values to its members.

5.1. The Model

Assume that an agent valuation of a DAO with M participants can be captured with a Ndimensional vector *x(t,M)* of 'component-evaluations' of the DAO in the positive real space $R^+x\ N \rightarrow R^N$ which captures the evolution of the DAO in time and in the number of participants. In a financial market this could be the valuation of a particular asset through clearing the supply and demand of securities. In a social network this could be a series of attributes, such as total activity, number of adverts consumed and total trade.

For each agent $i \in ...M$ there is a dimensional observed valuation vector which is a weighted sum of the state components, hence $y_i(t,M) = \omega(x(t,M), t,M)$, for a non-zero weighting function. For example ω could be static and exponential affine, i.e. $\omega(x(t,M), t,M) = exp(\omega' x(t,M))$ for a non-zero vector ω. This is a prototypical example in structured financial products.

Beside the valuation function we need also to consider the presence of potentially undesirable states, or Hazards in which DAO's evolution might be pushed by a number of malicious attackers $H < M$. The attackers have a corresponding *hazardous region H(t,M)* whereby H: $R^+x\ N \rightarrow R^N$ and such that if for some time t it is $\boldsymbol{x}(t,M) \in H(t,M)$ then $y_i(t,\boldsymbol{x}(t,M)) = 0$ for all $i = 1...M$. In other words when

the functional DAO state enters the region *H(t,M)*, the organization loses value to all participants. This is precisely what happened to 'The DAO' as we discussed in §4.

We make only a limited number of assumptions on the shape of this hazardous region (and the corresponding dual acceptable region). The first favourable assumption is that *H(t,M)* shrinks with time, i.e. $H(t,M) \supseteq H(t+\delta,M)$, as the designers and managers of the DAO fix bugs and push updates. A second favourable assumption is that the initial point of the domain $\boldsymbol{x}(0,M)$ is in the exterior of *H(0,M)* and the admissible region $R^N \setminus H(t,M)$ is a convex open set around $\boldsymbol{x}(0,M)$. This condition could be overly optimistic for particularly sophisticated (or most likely buggy, see Atzei et al. (2017)) contracts as there could be subsets of *H(t,M)* that are enclaves inside the acceptable region so that an acceptable trajectory between two acceptable points might traverse some potentially unacceptable states.

Our convexity conditions corresponds to the classical specification of security policies as specified by Schneider (2000) in which the legitimate execution is included into an envelope corresponding to the security policy and that can be guaranteed to stay within the region (if the security policy is decidable) by actually mediating any interaction of the DAO with external actors through general security monitor (Ngo et al. 2015) or, for only a very limited classes of programs, through mining behaviour (Jamrozik et al. 2016). Such envelope does not necessarily bound the acceptable evolution of the DAO[7]. A consequence of Schneider's widely accepted definition of security policy is that if for some τ we have $x(\tau,M) \in H(\tau,M)$ then for all $t \geq \tau$ we have $\boldsymbol{x}(t,M) \in H(t,M)$ and hence our definition of $R^N \setminus H(t,M)$ as a convex set.[8]

At this point we need to capture the potential evolution of the function considering the potential actions of the attackers. The presence of a Turing complete language to specify smart contracts that could dynamically join the nexus means that it is not technically possible to actually construct the envelope of a security monitor or even a rewriter of contracts on the fly that could enforce a security policy (Hamlen et al. 2006) able to constrain the DAO behaviour within the acceptable region. In other words, *by construction a general DAO is unruly*.

For example establishing an automatic test that would forbid the introduction into the DAO of

[7] Consider as a 2-D example the area between the horizontal axis and the horizontal line crossing the y axis at 1.

[8] The presence of potential enclaves of $H(t,M)$ could be technically addressed by edit automata (Ligatti et al. 2005) which are able to correct potentially bad evolution that can become eventually good. However, they would not change.

smart (sub)contract by individual users if they can be so that $y_i(t,\boldsymbol{x}(t,M)) \leq 0$ for some t would be in violation of Rice's theorem as we could construct a recursive distinguisher for two not-trivial sets of programs (See discussion on Footnote 3).

One could postulate that smart-contract developers could avoid using programming language features such as dynamic updates and reflection that would make the properties of the contracts undecidable and their behaviour unruly. All analysis of far less financially critical domains such a mobile apps or web sites have shown that developers have not restrained themselves from the use of dynamic, expressive features even when they would not need them (See for example Jensen et al. (2012) who quite appropriately joke about the 'evil' that 'eval', a Turing-complete but quite convenient construct, can wreak on the possibility of security analysis).

DAO designers could also use formal methods to certify smart-contracts before admitting them to the DAO to prove that they satisfy some desirable property[9]. Unfortunately, what is considered practical' in this domain would correspond to several days of analysis by large teams (See for example Acharya and Robinson (2011)), which would nullify the whole purpose of high speed distributed ledgers working at a speed of milliseconds as a way to automatically seize opportunities.

To consider the law of motion for $\boldsymbol{x}(t)$ we can work with a general Brownian Semi-Martingale of the following form: At this point we need to capture two possible evolutions: the one captured by honest users who actually performs their intended innovative activities and the one of malicious users who try to push the evolution of the DAO towards the hazard regions $H(t,M)$. In a distributed setting with sufficiently many actors M, it becomes impossible to distinguish possible evolution in which some actors push the state $\boldsymbol{x}(\tau,M)$ in a region where $y_i(t,\boldsymbol{x}(t,M)) = 0$ for some (or all) i by honest albeit unfortunate behaviour (See how in Massacci et al. (2017a), the authors went to a great extent to address the risk of broke traders for a simple financial product without smart contracts).

If an observer cannot likely tell a priori whether an action was innovative or malicious we can then model of innovative actions using the techniques suggest by Levinthal (1991) and Swaminathan (1996) to capture the evolution of the firm as well as its possible mortality. A natural solution in this setup is to capture movements in the RN as a random walk. Then, to capture the law of motion for $\boldsymbol{x}(t,M)$ we can consider the following decomposition:

[99] This is not in contrast with undecidability results: once the program is fixed, and no too expressive construct is present, its analysis is doable but might still take exponentially long.

$$\mathrm{d}x_j(t,M) = \underbrace{g_j(t,M)\mathrm{d}t}_{\text{Drift}} + \underbrace{\sigma_j(t,M)\mathrm{d}W(t)}_{\text{Continuous}} + \underbrace{\gamma_j(t,M)}_{\text{Jumps}}$$

for a component *j* where $W(t) - W(0) \sim \mathrm{N}(\mathbf{0}, tI)$ is, in its simplest form, a Weiner process for a *N* length null vector **0** and an identity matrix *I*. The drift function $g_j(t,M)$ may also be used to capture also potential discount factor that users may place on the evolution of the DAO. It is the 'intended' value at the time of inception. The stochastic function *W(t)* corresponds to the movements of good (or bad) actors that exploit the flexibility of the DAO to move it do a different space point (e.g. one where $y_i(\boldsymbol{x}(t+1,M), t, M) > y_i(\boldsymbol{x}(t,M), t, M)$ for some agent *i*. For simplicity in this treatment we will ignore jumps (which might corresponds to updates in functionalities) as the effect we want to measure is already present in their absence.

The high level of indeterminacy derived by the number of agents (each of whom can introduce potentially arbitrary smart contracts) can be easily captured by assuming that $\partial\sigma_j(t,M)/\partial M > 0$. So that for example $\sigma_j(t,M) \sim O(M^2)$ (for network and power law effects) or $\sigma_j(t,M) \sim O(e^M)$ for supermodular effects. The drift function might also depend on *M* as the value of the network might also have network or effects.

What can we say about hazard of the undesired functionality of the components when an increasing number of users enters the fray? First, clearly, as we increase the complexity, then the expected distance $|\boldsymbol{x}(t,M) - \boldsymbol{x}(0,M)|$ increases, therefore the volume of space covered in $\mathrm{R}^N \backslash H(t,M)$ increases.

It is then possible to prove that if the speed of expansion of *H(t,M)* is not sufficiently high in comparison to the variance of the random walk and *H* is sufficiently large then the process is inevitably going to hit the hazardous region with probability 1.

5.2. The simplest case: Weiner Process with knockout bound

From Itˆo calculus representation of a stochastic process, we know that if $y(t)=\omega(x(t))=x(t)$ and the state variable is one dimensional then: To extract a value for the DOA in the derivation below we assume that there is only one dimension to evaluate. Then, from Itˆo calculus, we know that if $y(t) = \omega(x(t))$ then:

$$\mathrm{d}y(t) = \left(\frac{\partial\omega}{\partial x(0)}g(x(0)) + \frac{\partial\omega}{\partial t} + \frac{1}{2}\frac{\partial^2\omega}{\partial x^2(0)}\sigma^2\right)\mathrm{d}t + \frac{\partial\omega}{\partial x(0)}\sigma\mathrm{d}W \qquad (1)$$

Hence the value function *y(t)* can be thought of as a commodity price that is a function of the community demand and the physical cost of generating the proof of swap within the virtual DAO community. Setting *g(x(t))=r* to be a positive constant rate of change in numéraire for which the assets within the DAO can be exchanged, then the simple:

$$\frac{\partial \omega}{\partial t} + \frac{\partial \omega}{\partial x(0)} r x(0) + \frac{1}{2} \frac{\partial^2 \omega}{\partial x^2(0)} \sigma_M^2 x^2(0) = r\omega \qquad (2)$$

The right-hand-side of the PDE provides the valuation benchmark, indeed, for organizations where the knockout is a more abstract process than a simple dollar valuation, this can be replaced some other function, but for this simple illustration we will adhere to the standard interpretation that the organisation is valued against a complete market.

A further simplifying assumption is that the evolution of patches is actually discrete and significantly slower than the pace of evolution which would be consistent with both theoretical models of patching strategies (see for example Cavusoglu et al. (2008)) and empirical models of attacks and countermeasures of IS (Ransbotham and Mitra 2009, August and Tunca 2011). Then we can assume that during the a period of evolution of x(t,M) the hazard region is essentially constant and therefore $H(t,M) = [h,\infty]$ for some $h \in \mathbb{R}_+$. Therefore the boundary condition becomes $x(t) \geq h$, $y(t)=0$, for some perpetual time frame.

If we approximate the functional form of $\omega(x(t)) = x(t)^{\alpha}$ then the present value of holding y(t) will be a solution of the form $\frac{1}{2}\sigma^2\alpha(\alpha-1)+r\alpha-r=0$, solved simultaneously with the PDE. This yields the result that when $x(0)<h$, we obtain the following valuation condition:

$$y(0) = h\left(1 - \frac{\xi}{1-\xi}\right)\left(1 - \frac{1+\xi x(0)}{1+\xi h}\right)^{-\xi} \quad \xi = 2r/\sigma_M^2 \qquad (3)$$

As we can see if $\lim M \to \infty$ the valuation of *y* goes to zero as $\lim \sigma_M \to \infty$ corresponding to the intuition that with too many users it is essentially certain that the evaluation of *y(t)* will basically hit the hazard boundary sooner than later. However, this might be obfuscated for the initial smaller values of *M* by a large value of the drift value *r*. However, as the variance is squared, the random walk effect will eventually overwhelm the drift effect as *M* grows when more users join, this is illustrated in Figure 4. Notice that this is materially different from standard real option valuation models with knock outs where the intrinsic valuation of the implicit contract monotonically varies

with the state asset with the lowest positive value when state variable approaches the bound.

However, in this case the highest value of the DAO is just prior to the hazard bound.

5.3. Jump diffusion in two dimensions with curved hazard geometries

Clearly, the simplest form provides an intuitive representation of the different cases, but are unrealistic for anything but trivial value processes. Unfortunately, geometrically, most cases can only be solved by simulation and a further complication is that the hazard domain is not easily described (indeed for most Turing complete scripting languages it is impossible, by definition, to describe at inception).

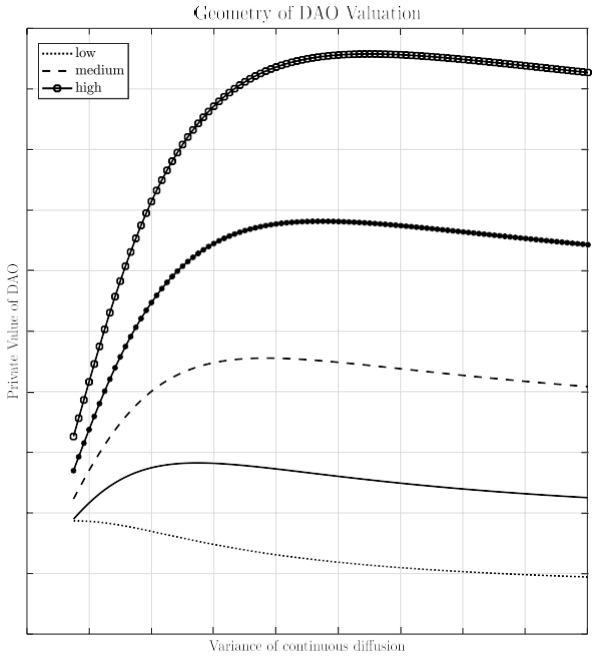
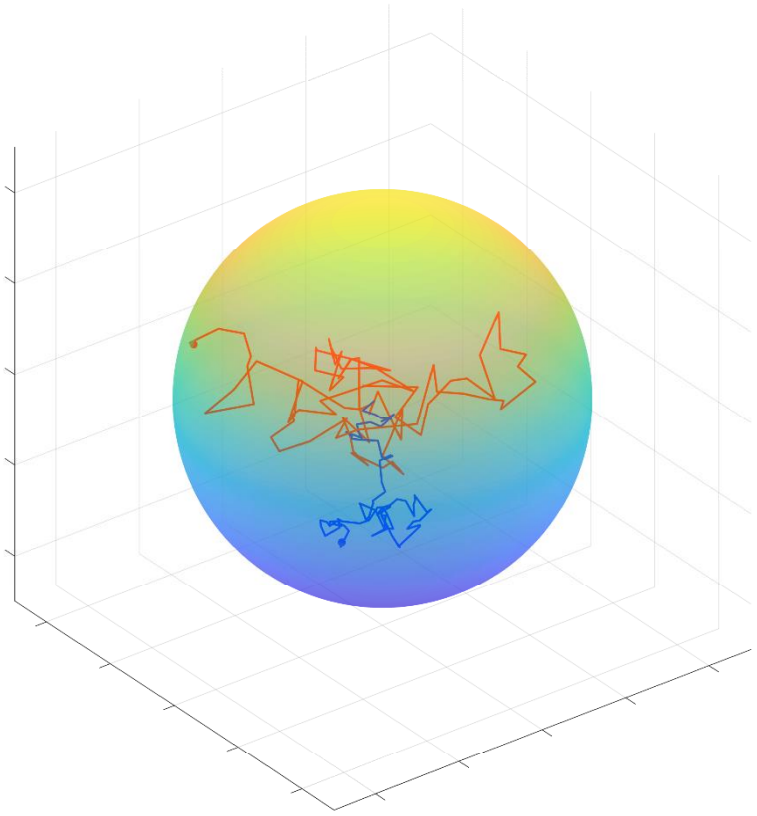


Figure 4 Illustration of the expected private value of the DAO at inception *y(0)* with an upper knock-out bound. Here the DAO value *y(t)* is *x(t)* unless *x(t)*≥ *h* and then *y(t) = 0*. The owner of the contract is presumed to be able to liquidate the position at any time *t*, unless *x(s)*≥ *h*, then *y(t) = 0*, for *t > s*.

In Figure 5, we show two different simulations for the two dimensional case of ***x(t,M)***. The hazard region of the components lies outside the unit circle and it is assumed to be relatively stationary (or move very slowly) during the observation period. We consider two possible diffusions with small discrete steps. The first (the blue line) has a lower continuous variance (a smaller number of participants), and the second, the red-line, with the same jump size and number of jump steps but larger continuous variance an If the number of participants is an itself an attractor for a much larger number of participants to flock in $(\partial M/\partial t \sim O(M))$, then the variance of the DAO's evolution increases super-linearly and the probability of hitting the hazard region increases. In contrast, the

possibility of pushing updates is normally slowed down by the number of users $(\partial^2\mathcal{H}/\partial t\partial M < 0)$ as the DAO operators need to make sure the increasingly diverse number of legitimate users is not affected by the updated.

Figure 5 Two Alternative Hazard Behaviors for Different Participants



Note. Any point inside the sphere represent an acceptable status of the DAO. The red line is a possible system evolution. It has a large number of users and traverses the boundary after only a small number of iterations. The blue line has a lower variance (i.e. significantly less participants) and takes longer to avoid contact so that the hazard region could expand by security patching or deployed countermeasures.

6. Concluding Remarks

We argue that distributed ledger technologies (DLTs), block-chains and cryptographically enabled contracts (CryptoECs) are more than simply a disruptive technology for the financial sector replacing existing networks. Critically, we introduce a new notion to sit behind radical innovation, disruptive innovation and modular technologies. The notion of unruly innovation is that of an underlying economic framework, for which a hyper-disruptive technology essentially changes the complete economic architecture upon which organizations are built. This argument complements the existing models of disruption and radical innovation synchronizing these concepts with the economic concept of combinatorial innovation and super-modularity. A core characteristic of this type of disruption (which we refer to as 'changing the game', following the game theoretic insight) is that extremely

low fixed costs result in gradual adoption even if the social welfare paradigm seeks to place blocks in its path. This extremely low adoption cost is coupled with a gradual migration that is essentially irreversible, hence once the game has changed incumbents disappear.

Furthermore, we have illustrated that the technology envisioned has several drawbacks that might motivate a social planner intervention, most notably the inherent redundancy of the social planner itself as it is inherently excluded from the economic interactions having been replaced by the ledger. With this disappearance that are significant side-effects that might be viewed as detrimental, most notably the lack of discretion in Tort based remediation of contractual disputes. This is a result of the code providing no recourse other than that which the algorithm dictates given the state of any input variables.

Attempts to change the ledger to redress a tort may then be seen by some of the members of the community to change the very basic principles of a DLTs with CryptoECs and then can be resisted upfront by refusing to join the new "redressed" ledger thus yielding to a "Balkanization" of the market. In the words of Ethereum Classic's Declaration of Independence:

> *Ultimately, these breaches in fungibility and immutability were made possible by the subjective morality judgements of those who felt a burning desire to bring the alleged attacker to justice. However, in doing so they compromised a core pillar of Ethereum just to do what they felt was in the interests of the "greater good". In a global community where each individual has their own laws, customs, and beliefs, who is to say what is right and wrong?*

The desire of modern firms to capture information and process ideas in a flexible manner by the underpinning contracts will inevitably exhibit sufficient computational complexity that may prevent careful forecasting of potential future states. The absence of a social authority to mitigate the extreme trajectories of markets dominated by unruly innovation might then yield less-than-desirable and surely far-from-predictable outcomes.

References

Acharya, Mithun, Brian Robinson. 2011. Practical change impact analysis based on static program slicing for industrial software systems. Proc. of the 33rd Int. Conf. on Software Engineering (ICSE'11).

Adner, Ron. 2002. When are technologies disruptive? a demand-based view of the emergence of competition. Strategic Management Journal 23(8) 667–688. URL http://www.jstor.org/stable/3094287.

Alford, Robert R. 1977. Health care politics: Ideological and interest group barriers to reform. University of Chicago Press.

Atzei, Nicola, Massimo Bartoletti, Tiziana Cimoli. 2017. A survey of attacks on ethereum smart contracts (sok). International Conference on Principles of Security and Trust . Springer, 164–186.

Atzei, Nicola, Massimo Bartoletti, Tiziana Cimoli, Stefano Lande, Roberto Zunino. 2018. Sok: unravelling bitcoin smart contracts. International Conference on Principles of Security and Trust. Springer, 217–242.

August, Terrence, Tunay I Tunca. 2011. Who should be responsible for software security? a comparative analysis of liability policies in network environments. Management Science 57(5) 934–959.

Bank of England. 2015. One bank research agenda. http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf. Accessed: 2015-12-30.

Bartoletti, Massimo, Livio Pompianu. 2017. An empirical analysis of smart contracts: platforms, applications, and design patterns. International Conference on Financial Cryptography and Data Security. Springer, 494–509.

Ben-Or, Michael. 1983. Another advantage of free choice (extended abstract): Completely asynchronous agreement protocols. Proceedings of the second annual ACM symposium on Principles of distributed computing. ACM, 27–30.

Binmore, Ken. 2007. Playing for real: a text on game theory. Oxford university press.

Biryukov, Alex, Dmitry Khovratovich, Ivan Pustogarov. 2014. Deanonymisation of clients in bitcoin p2p network. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.ACM, 15–29.

Bitcoin Wiki. 2015a. Bitcoin mt. gox. https://en.bitcoin.it/wiki/Mt._Gox. Accessed: 2015-12-30.

Bitcoin Wiki. 2015b. Bitcoin proof of stake. https://en.bitcoin.it/wiki/Proof_of_Stake. Accessed: 2015-12-30.

Bitcoin Wiki . 2015c. Bitcoin proof of work. https://en.bitcoin.it/wiki/Proof_of_work. Accessed: 2015-12-30.

Bitcoin Wiki . 2015d. Bitcoin wallet. https://en.bitcoin.it/wiki/Wallet. Accessed: 2015-12-30.

Bonneau, J., A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten. 2015. Sok: Research perspectives and

challenges for bitcoin and cryptocurrencies. Security and Privacy (SP), 2015 IEEE Symposium on. 104–121.

Callon, Michel, ed. 1998. The laws of the markets. Blackwell Publishers/Sociological Review.

Callon, Michel, Fabian Muniesa. 2005. Peripheral vision: Economic markets as calculative collective devices. Organization studies 26(8) 1229–1250.

Castro, Miguel, Barbara Liskov. 2002. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS) 20(4) 398–461.

Castro, Miguel, Barbara Liskov, et al. 1999. Practical byzantine fault tolerance. OSDI , vol. 99. 173–186.

Cavusoglu, Hasan, Huseyin Cavusoglu, Jun Zhang. 2008. Security patch management: Share the burden or share the damage? Management Science 54(4) 657–670. doi:10.1287/mnsc.1070.0794. URL http: //dx.doi.org/10.1287/mnsc.1070.0794.

Cetina, Karin Knorr, Alex Preda. 2007. The temporalization of financial markets: From network to flow. Theory, Culture & Society 24(7-8) 116–138.

Chaum, David. 1982. Blind signatures for untraceable payments. Advances in cryptology. Springer, 199–203.

Chaum, David, Amos Fiat, Moni Naor. 1990. Untraceable electronic cash. Proceedings on Advances in cryptology. Springer-Verlag New York, Inc., 319–327.

Christensen, Clayton M. 1993. The rigid disk drive industry: a history of commercial and technological turbulence. Business history review 67(04) 531–588.

Christensen, Clayton M, Michael E Raynor. 2003a. Why hard-nosed executives should care about management theory. *Harvard business review* **81**(9) 66–75.

Christensen, Clayton M, Michael E Raynor. 2003b. *The Innovator's Solution: Creating and Sustaining Successful Growth*. Harvard Business Press.

Christensen, Clayton M, Fernando F Su´arez, James M Utterback. 1998. Strategies for survival in fast changing industries. Management science 44(12-part-2) S207–S220.

Christensen, Thomas J, Jack Snyder. 1997. Progressive research on degenerate alliances. American Political Science Review 91(04) 919–922.

Coad, Alex, Julian Frankish, Richard G Roberts, David J Storey. 2013. Growth paths and survival chances: An application of gambler's ruin theory. Journal of Business Venturing 28(5) 615–632.

Dai, Wei. 1998. b-money. http://www.weidai.com/bmoney.txt. Accessed: 2015-12-30.

Danezis, George, Sarah Meiklejohn. 2015. Centrally banked cryptocurrencies. Tech. rep., University College London.

Danneels, Erwin. 2004. Disruptive technology reconsidered: A critique and research agenda. Journal of product innovation management 21(4) 246–258.

Decker, Christian, Roger Wattenhofer. 2014. Bitcoin transaction malleability and mtgox. Computer Security-ESORICS 2014 . Springer, 313–326.

Denrell, Jerker. 2004. Random walks and sustained competitive advantage. Management Science 50(7) 922–934.

DeTienne, Dawn R, Dean A Shepherd, Julio O De Castro. 2008. The fallacy of "only the strong survive": The effects of extrinsic motivation on the persistence decisions for under-performing firms. Journal of Business Venturing 23(5) 528–546.

Ducy, Patricia, Michael Amling, Shu Takeda, Matthias Priemel, Arndt F Schilling, Frank T Beil, Jianhe Shen, Charles Vinson, Johannes M Rueger, Gerard Karsenty. 2000. Leptin inhibits bone formation through a hypothalamic relay: a central control of bone mass. Cell 100(2) 197–207.

Ethereum. 2015. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed: 2015-12-30.

Eyal, Ittay, Emin G¨un Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. Financial Cryptography and Data Security. Springer, 436–454.

Finney, Hal. 2004. Rpow - reusable proofs of work. https://cryptome.org/rpow.htm. Accessed: 2015-12-30.

Fleder, Michael, Michael S. Kester, Sudeep Pillai. 2015. Bitcoin transaction graph analysis. CoRR abs/1502.01657 1–8. URL http://arxiv.org/abs/1502.01657.

Florida, Richard L, Martin Kenney. 1990. The breakthrough illusion: Corporate America's failure to move from innovation to mass production. Basic Books (AZ).

Gersick, Connie JG. 1991. Revolutionary change theories: A multilevel exploration of the punctuated equilibrium paradigm. Academy of management review 16(1) 10–36.

Gimeno, Javier, Timothy B Folta, Arnold C Cooper, Carolyn Y Woo. 1997. Survival of the fittest? Entrepreneurial human capital and the persistence of underperforming firms. Administrative science quarterly 750–783.

Govindarajan, Vijay, Praveen K Kopalle. 2006. The usefulness of measuring disruptiveness of innovations ex post in making ex ante predictions. Journal of product innovation Management 23(1) 12–18.

Hamlen, Kevin W., Greg Morrisett, Fred B. Schneider. 2006. Computability classes for enforcement mechanisms. ACM Trans. Program. Lang. Syst. 28(1) 175–205.

Hannan, Michael T, John Freeman. 1984. Structural inertia and organizational change. American sociological review 149–164.

Harris, Larry. 2003. Trading and exchanges: Market microstructure for practitioners. Oxford University Press.

Henderson, Rebecca M, Kim B Clark. 1990. Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms. Administrative science quarterly 9–30.

Jakobsson, Markus, Ari Juels. 1999. Proofs of work and bread pudding protocols (extended abstract). Secure Information Networks, IFIP — The International Federation for Information Processing, vol. 23. Springer US, 258–272. doi:10.1007/978-0-387-35568-9 18.

Jamrozik, Konrad, Philipp von Styp-Rekowsky, Andreas Zeller. 2016. Mining sandboxes. Proceedings of the 38th International Conference on Software Engineering. ICSE '16, ACM, New York, NY, USA, 37–48. doi:10.1145/2884781.2884782. URL http://doi.acm.org/10.1145/2884781.2884782.

Jensen, Simon Holm, Peter A Jonsson, Anders Møller. 2012. Remedying the eval that men do. Proceedings of the 2012 International Symposium on Software Testing and Analysis. ACM, 34–44.

Karame, Ghassan O, Elli Androulaki, Srdjan Capkun. 2012. Double-spending fast payments in bitcoin. Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 906–917.

Karame, Ghassan O, Elli Androulaki, Marc Roeschlin, Arthur Gervais, Srdjan ˇCapkun. 2015. Misbehavior in bitcoin: A study of double-spending and accountability. ACM Transactions on Information and System Security (TISSEC) 18(1) 2.

Karim, Samina. 2006. Modularity in organizational structure: The reconfiguration of internally developed and acquired business units. Strategic Management Journal 27(9) 799–823.

Koshy, Philip, Diana Koshy, Patrick McDaniel. 2014. An analysis of anonymity in bitcoin using p2p network traffic. Springer.

Langlois, Richard N, Paul L Robertson. 1992. Networks and innovation in a modular system: Lessons from the microcomputer and stereo component industries. Research Policy 21(4) 297–313.

Lessig, Lawrence. 1999. Code is law. The Industry Standard 18.

Lessig, Lawrence. 2009. Code: And other laws of cyberspace. ReadHowYouWant.com.

Levinthal, Daniel A. 1991. Random walks and organizational mortality. Administrative Science Quarterly 397–420.

Ligatti, Jay, Lujo Bauer, David Walker. 2005. Edit automata: Enforcement mechanisms for run-time security policies. International Journal of Information Security 4(1-2) 2–16. doi:10.1007/s10207-004-0046-8.

Lynch, Nancy. 1989. A hundred impossibility proofs for distributed computing. Proceedings of the eighth annual ACM Symposium on Principles of Distributed Computing. ACM, 1–28.

MacKenzie, Donald. 2008. An engine, not a camera: How financial models shape markets. MIT Press.

Markides, Constantinos. 2006. Disruptive innovation: In need of better theory. Journal of product innovation management 23(1) 19–25.

Massacci, Fabio, Chan Nam Ngo, Jing Nie, Daniele Venturi, Julian Williams. 2017a. Futuresmex: Secure, distributed futures market exchange. FuturesMEX: Secure, Distributed Futures Market Exchange. IEEE, 0.

Massacci, Fabio, Chan Nam Ngo, Jing Nie, Daniele Venturi, Julian Williams. 2017b. The seconomics (security-economics) vulnerabilities of decentralized autonomous organizations. Cambridge International Workshop on Security Protocols. Springer, 171–179.

Massacci, Fabio, Chan-Nam Ngo, Julian M Williams. 2016. Decentralized transaction clearing beyond blockchains. Available at SSRN: https://ssrn.com/abstract=2794913.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geo↵rey M Voelker, Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. Proceedings of the 2013 conference on Internet measurement conference. ACM, 127–140.

Miers, Ian, Christina Garman, Matthew Green, Aviel D Rubin. 2013. Zerocoin: Anonymous distributed e-cash from bitcoin. Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 397–411.

Miller, Daniel. 2002. Turning callon the right way up. Economy and society 31(2) 218–233.

Morone, Joseph G. 1993. Winning in high-tech markets: The role of general management. Harvard Business Press.

Nakamoto, Satoshi. 2008. Bitcoin: A peer-to-peer electronic cash system. Tech. rep., Unknown.

Ngo, Minh, Fabio Massacci, Dimiter Milushev, Frank Piessens. 2015. Runtime enforcement of security policies on black box reactive programs. Proceedings of the 42Nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. POPL '15, 43–54. doi:10.1145/2676726.2676978. URL http://doi.acm.org/10.1145/2676726.2676978.

Ober, Micha, Stefan Katzenbeisser, Kay Hamacher. 2013. Structure and anonymity of the bitcoin transaction graph. Future internet 5(2) 237–250.

Percival, Colin. 2009. Stronger key derivation via sequential memory-hard functions. Self-published.

Perritt, HH. 2000. Lawrence lessig, code and other laws of cyberspace. Connecticut Law Review 32(3) 1061–1064.

Ransbotham, Sam, Sabyasachi Mitra. 2009. Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research 20(1) 121–139. doi:10.1287/isre.1080.0174.

Reid, Fergal, Martin Harrigan. 2013. An analysis of anonymity in the bitcoin system. Springer.

Ripple Labs. 2015. Executive summary for financial institutions. https://ripple.com/solutions/ executive-summary-for-financial-institutions/. Accessed: 2015-12-30.

Ripple Lab. 2015a. Gateway guide. https://ripple.com/build/gateway-guide/. Accessed: 2015-12-30.

Ripple Labs. 2015b. Market makers. https://ripple.com/knowledge_center/market-makers-2/.Accessed: 2015-12-30.

Ripple Labs. 2015c. Order book. https://ripple.com/knowledge_center/explaining-the-order-book-and-trading-currency/. Accessed: 2015-12-30.

Ripple Labs. 2015d. Payment paths. https://ripple.com/build/paths/. Accessed: 2015-12-30.

Ron, Dorit, Adi Shamir. 2013. Quantitative analysis of the full bitcoin transaction graph. Financial Cryptography and Data Security. Springer, 6–24.

Ron, Dorit, Adi Shamir. 2014. How did dread pirate roberts acquire and protect his bitcoin wealth? Financial Cryptography and Data Security. Springer, 3–15.

Rosenfeld, Meni. 2014. Analysis of hashrate-based double spending. Tech. rep., Unknown.

Sanchez, Ron, Joseph T Mahoney. 1996. Modularity, flexibility, and knowledge management in product and organization design. Strategic management journal 17(S2) 63–76.

Schilling, Melissa A, H Kevin Steensma. 2001. The use of modular organizational forms: An industry-level analysis. Academy of Management Journal 44(6) 1149–1168.

Schneider, Fred B. 2000. Enforceable security policies. ACM Trans. Inf. Syst. Secur. 3(1) 30–50. doi: 10.1145/353323.353382.

Schumpeter, Joseph. 1942. Creative destruction. Capitalism, socialism and democracy 82–5.

Securities and Exchange Commission. 2014. Sec charges NYSE, NYSE ARCA, and NYSE MKT for repeated failures to operate in accordance with exchange rules. https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541706507.

Sipser, Michael. 2012. Introduction to the Theory of Computation. Cengage Learning.

Spulber, Daniel F. 1996. Market microstructure and intermediation 10(3) 135–152.

Swaminathan, Anand. 1996. Environmental conditions at founding and organizational mortality: A trial-by-fire

model. Academy of management journal 39(5) 1350–1377.

Szabo, Nick. 2005. Bit gold. http://unenumerated.blogspot.it/2005/12/bit-gold.html. Accessed: 2015-12-30.

Tellis, Gerard J. 2006. Disruptive technology or visionary leadership? Journal of Product Innovation Management 23(1) 34 – 38. URL http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=19203518&site=ehost-live.

Tiwana, Amrit. 2008. Does technological modularity substitute for control? a study of alliance performance in software outsourcing. Strategic Management Journal 29(7) 769–780.

Yu, Dan, Chang Chieh Hang. 2010. A reflective review of disruptive innovation theory. International Journal of Management Reviews 12(4) 435–452. doi:10.1111/j.1468-2370.2009.00272.x. URL http://dx.doi.org/10.1111/j.1468-2370.2009.00272.x.

Zenger, Todd R, William S Hesterly. 1997. The disaggregation of corporations: Selective intervention, high powered incentives, and molecular units. Organization Science 8(3) 209–222.

Appendix. Internet Compendium of Components of DLT For Payment Transaction Networks

Following the history of the cryptocurrency PTNs, we can highlight 4 major categories.

A. Digital cash PTNs (E-cash)

The history of cryptocurrency PTNs can be dated back to David Chaum's E-cash scheme (Chaum 1982). The PTN protocol for E-cash can be described in a simplified way as follows.

1. Clients deposit some money at the bank that support E-cash.
2. A payer send a serial number to the E-cash bank where the bank sign a Blind Signature on the serial number and debit the corresponding value from the payer's account.
3. A payer, upon payment, will give the payee the serial number.
4. The payee sends the serial number for verification at the bank.
5. Upon successful validation, the bank will credit the corresponding value to the payee's account and mark the serial number as spent.

The noteworthy features of the E-cash scheme is the anonymity level it provides. Even the cooperation between the bank and the payee would still not be able to identify the payer, all thanks to the Blind Signature technology that the scheme applies. However, it is still a form of converting a physical token into a digital one and there is only one central authority that maintains the ownership of the tokens.

B. Blockchain based PTNs (Bitcoin)

Subsequent attempts at a purely digital currency were B-Money (Dai 1998), hashcash (Finney 2004), and BitGold (Szabo 2005) which initially utilize "Proof-of-Work" (Jakobsson and Juels 1999), a hard cryptographic computational puzzle, as a mean of determining the inherent value for the medium of exchange (in Bitcoin). Later, the Bitcoin network, combining with a vast of research results in distributed systems, digital time-stamping, and cryptography, has brought about the most successful cryptocurrency in history so far. It is also worth to note that the Bitcoin approach is completely free of a central bank. The applications of Proof-of-Work and Blockchain are the core components that allow Bitcoin to be decentralized.

Proof-of-Work provides the Bitcoin network's users the capability to deposit value into the network. By solving a Proof-of-Work, the so-called "miner" will be rewarded with some Bitcoin. The Proof- of-Work is also a mechanism to prevent any attempt to revert a transaction that is already included in the blockchain.

Blockchain is a sequence of applications of a hash function to a sequence of transactions. Every block contains

the information of the current transaction and a references to its previous block header's hash. Ultimately, it will lead to the first block ever created, the Genesis block. The blockchain is shared by all nodes of the network and every transactions are stored within the blockchain so that it is transparent for everyone to know the balance of each account in the network.

C. Bitcoin-esque PTNs

Since the launch of Bitcoin in 2009, various Bitcoin-esque cryptocurrencies have been developed to solve several practical issues of the network.

- Some of them use different hash functions. Litecoin and PotCoin utilize a memory-costly hash function (Percival 2009) to deter the use of hardware-based mining devices.
- Some others try to improve the PTN's scalability, e.g. BlackCoin and Nxt apply the Proof-of-Stake mechanism (Bitcoin Wiki 2015b) where the miners need to prove the ownership of a certain amount of cryptocurrency to improve throughput. Ripple (Ripple Labs 2015), on the other hand, applies the Byzantine Fault Tolerant algorithm by (Castro et al. 1999) to agree on a commit.
- Anonymity and privacy are also noticeable issues of the Bitcoin network's design. ZeroCoin (Miers et al. 2013) is a combination of the E-cash scheme and Bitcoin to improve Bitcoin's anonymity. Subsequently, the ZeroCoin approach was implemented as Moneta.
- One of the primary concerns that central banks may have is losing control of money-supply as an instrument of policy. The RSCoin (Danezis and Meiklejohn 2015) approach is a Bitcoin extension which answers the call of the Bank of England's research agenda (Bank of England 2015). The network delegates the monetary supply to a central authority, such as a bank, but utilizes a distributed network of other parties to perform transaction validation. However, as doing so, the network introduce a central point of failure which Bitcoin has tried to prevent. The central bank is still on top of the hierarchy and maintains the ultimate ledger.

D. Decentralized Autonomous Organizations (Ethereum)

Many of the new cryptocurrencies above also try to offer extended functionality. At an extreme this is represented by Ethereum which claims a “programming languages for financial contracts".

“A built-in fully edged Turing-complete programming language that can be used to create “contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code" (Ethereum 2015).

Table 4 Terms & Descriptions

Balance Database	The database that keeps the balance of customers in a financial institution.
Blockchain	An online, distributed and append only ledger that needs an consensus algorithm to maintain its integrity.
Blind Signature	The scheme that e-cash model uses to sign the Serial Number without knowing the content. The banks that support e-cash can have multiple signing key each of which assign a different value to the signed Serial Number (Chaum 1982)
Deanonymization	Although the distributed PTNs often offer anonymity in coins ownership and payment, the attacker has a chance to group and link the coins back to the owner by different methods (Koshy et al. 2014, Biryukov et al. 2014, Reid and Harrigan 2013, Fleder et al. 2015, Ron and Shamir 2013, Meiklejohn et al. 2013, Ron and Shamir 2014, Ober et al. 2013).
Exchanger	A third-party organization that provide exchange for the digital currency and another currency such as commodity, fiat or another digital currency (Bitcoin Wiki 2015a).
Fork	In a blockchain, a fork happens when more than one node sends the solution for the PoW. In this case, the nodes will keep track of all the forked blocks while working towards the next block. In the end, only one block will be kept in the main chain.
Gateway	The financial institution, e.g. bank, that provides liquidity to the Ripple network. A gateway usually keeps a cold wallet, which it uses to issue the issuances, and a hot wallet, which it uses to sign the transactions in the network (Ripple Labs 2015a).
Issuance	A representation of another currency, as long as it has some value and is exchangeable, in the Ripple network. An issuance is bound to an issuer. The currency that an issuance represent can cover other digital currencies such as Bitcoin, etc. as well as current real-world fiat currency, e.g. USD, EUR. It can also represent the virtual currency such as flight miles (Ripple Labs 2015a).
Majority attack	When the malicious clients control the majority of the computational power, they can rewrite the transaction history (Nakamoto 2008, Rosenfeld 2014).
Malleability	Refers to an implementation flaw that allows the modifications in the transaction data without changing the hash value of the block header (Decker and Wattenhofer 2014).
MarketMaker	The Ripple client that offers the bid/ask orders to exchange from currency to currency (Ripple Labs 2015b).
Off-chain settlement	The transactions are not all settled on the blockchain but some of them are aggregated in another network and then settled the net amount on the blockchain later (Bonneau et al. 2015).
OrderBook	The database that keeps track of bid/ask orders from MarketMakers (Ripple Labs 2015c).
PathFinding	The algorithm that automatically finds an exchange path for a payment in Ripple network that involves currency exchange using the OrderBook (Ripple Labs 2015d).
Public Key	A public key, usually hashed, can serve as a destination address of a payment. This takes the role of a pseudonym to protect user privacy in the distributed PTNs.
Private Key	A private key that is used to unlock the fund upon receiving at the Public Key address.
Proof-of-Work	A hard to solve but easy to verify puzzle, is used to prevent Denial-of-Service in distributed PTNs (Bitcoin Wiki 2015b).
Selfish-mining	In the Bitcoin network, the number of block contribution to the main chain of a node should be proportional to its computational power. Selfish-mining is an attack on the block mining mechanism that allows unfair block distribution (Eyal and Sirer 2014).
Serial Number	The string that is kept secret to the owner, later the Serial# can be used to prove the ownership of the digital coin.
Spent Serial Number Database	The database that keeps track of the spent secrets. In e-cash model, the e-cash bank has to collect all the spent Serial Number to prevent them from being used twice.
Transaction Fee	The transaction fee that is used as incentives for the distributed nodes working towards adding transactions into the blockchain.
Unspent-Transaction-Output	In a blockchain, the UTXO is the output of a previous transaction that has never been used as an input in another transaction. The UTXO is referenced by a tuple of previous transaction ID and the output’s index. To unlock the fund in the output, the owner has to provide the correspondent private key.

Wallet	A collection of secrets(Serial Number, Private Key, etc.) to prove ownership of a specific digital coin (Bitcoin Wiki 2015c, Chaum et al. 1990).
Zero-confirmation	In the case of Bitcoin for fast-payment when the merchant cannot wait for even one confirmation (10 minutes average), the merchant suffers from the double-spending attack where the attacker broadcast two transactions: one to pay the merchant and another one to pay oneself with the same unspent outputs. The merchant will receive no fund if the latter transaction is confirmed first (Karame et al. 2012, 2015).